디지털산업정보학회 논문지 제15권 제1호-2019년 3월
https://doi.org/10.17662/ksdim.2019.15.1.053

HTTPS 웹 사이트 차단의 익명성 제공 방안 연구

김 태 경*

Study on Providing Anonymity of HTTPS Web Site Blocking

Kim Taekyung

〈Abstract〉

As the number of harmful sites increases, many social problems are occurring. Therefore, in order to solve this problem, the government is carrying out activities to block access to web sites to harmful sites based on the law. However, due to the change from HTTP to HTTPS protocol, it has become difficult to block the harmful sites in the existing method. In the existing HTTP protocol, a method of blocking the site corresponding to the harmful site domain list by utilizing the DNS information was used. However, due to the generalization of HTTPS, it is difficult to block the harmful sites in the existing method. Therefore, the ISP uses the method of blocking the website using the SNI field in the TLS (Transport Layer Security) Handshake protocol used for HTTPS.

However, since the method using SNI field raises the concern of monitoring Internet users or exposing information about connected sites, in this paper, we proposed method which can support anonymity to Internet users while blocking harmful sites. The suggested method also can support integrity and source authentication to the transmitted data.

Key Words : HTTP, HTTPS, SNI, TLS, Site Blocking

Ⅰ. 서론

온라인 불법 도박 시장 규모가 점차 확대되고 있으며, 도박이 국경 없는 온라인에서 해외 사이트를 통해 심각한 폐해를 낳고 있을 뿐 아니라 불법촬영물, 이른바 몰카로 인한 피해가 증가함에 따라 정부에서도 이러한 콘텐츠들을 차단하기 위한 방안들을 고려하고 있다. 더구나 기술 변화에 따라 보안이 강화되면서 HTTPS가 확산되면서 HTTP 프로토콜이 주로 사용되었던 시기의 방식으로는 불법 촬영물이 있는 해외 불법 사이트 차단이 어려워졌다. 따라서 이러한 사이트를 차단하기 위해 SNI(Server Name Indication) 필드를 이용한 웹사이트 차단 기술이 도입되었다. 이 기술은 서버 네임이 불법 사이트와 일치하면 기계적으로 접속을 차단하는 방식이다. 그러나 이러한 사이트 차단방식은 인터넷 사용자들에 대한 감시 혹은 접속하는 사이트에 대한 정보노출 이라는 이슈가 제기되고 있다. 현재 웹사이트에 대한 차단은 우리나라뿐만 아니라 다른 나라에서도 저작권 및 정치적 이유 등 여러 가지 이유로 웹사이트 차단 정책을 실행하고 있다[1, 2].

* 명지전문대학 인터넷응용보안공학과 교수

기존에 불법 인터넷 사이트에 대한 차단은 warning.or.kr의 사이트를 통해 수행되어 왔다. 이런 불법 사이트들에 대한 차단은 기본적인 정보통신과 관련된 법[3]에서 음란물을 불법으로 하는 규정을 근거로 하고 있다. 인터넷에서는 HTTP(Hyper Text Transfer Protocol)를 이용하여 평문으로 데이터를 송수신하고 있다. 그러나 HTTP 데이터[4]는 데이터를 캡처하면 해당 내용이 무엇인지 분석이 가능하므로 보안성을 높이기 위해 HTTP 대신에 대부분의 사이트에서 HTTPS[5, 6]를 사용하고 있다. HTTPS는 브라우저와 서버간 주고받는 데이터를 암호화하여 전송하기 때문에 비교적 안전하게 인터넷 통신을 수행할 수 있다. 그러나 인터넷 사용자가 접속하려는 웹사이트의 유해 사이트 여부를 판별하기 위해서는 어느 사이트에 접속하는지 암호화된 데이터를 복호화 해야 하는데, 암호화키를 알 수 없으므로 해당 내용을 복호화 할 수 없으므로 정부에서는 SNI 필드를 이용한 유해사이트 차단 방식을 고려하게 되었다.

SNI 필드를 이용한 유해사이트 차단은 2019년 2월 11일 KT를 시작으로 시작되었다. 또한 2월 12일에는 SKT 및 SKB에서도 SNI를 이용한 유해사이트 차단이 적용되었으며 추후 모든 ISP에 적용하기로 하였다. SNI 필드 정보는 이전에도 평문으로 전송되었고 이를 이용하여 웹사이트 차단을 수행하지 않아 보안 강화의 측면에서만 연구가 수행되었으나 이 정보를 이용한 사이트 차단 정책의 실행으로 인터넷 사용자들이 방문하려는 사이트 정보의 노출 등의 이슈가 발생하게 되었다.

따라서 본 논문에서는 유해 사이트를 안전하게 차단하되 익명성을 제공함으로 개인정보를 보호할 수 있는 방법에 대한 연구를 수행하고자 한다.

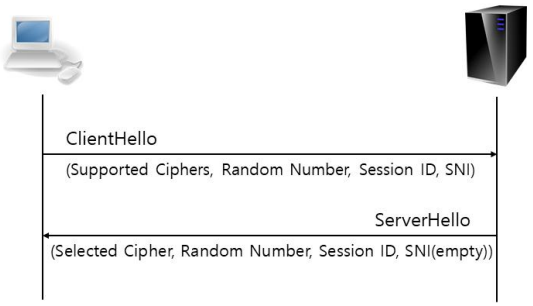
본 논문의 2장에서는 HTTPS의 SNI에 대해서 관련 내용을 제시하였으며, 3장에서는 익명성을 제공할 수 있도록 하는 유해 사이트 차단모델의 제시 및 분석을 수행하였다. 마지막으로 4장에서는 본 연구의 결론으로 구성하였다.

Ⅱ. 관련연구

2.1 SNI 개념

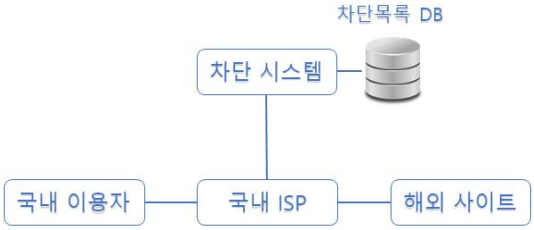
SNI는 Server Name Indication의 약어로 이 필드는 이용자가 보안 접속을 통해 해외불법사이트에 접속할 때 사용하는 암호화되지 않은 영역이다. 이 기술이 나오게 된 이유는 하나의 웹서버가 여러 웹사이트를 서비스하면서 인증서 인증에 문제가 생겼기 때문이다. 기존까지는 대상 서버의 IP 주소와 도메인이 1:1 대응 관계라서 서버의 인증서 제공에 문제가 없었지만, 여러 도메인을 하나의 IP 주소로 연결하는 서비스가 대중화되면서 보낼 인증서를 특정하지 못하게 되었다. 이 때문에 클라이언트가 사이트에 접속하면서 도메인 정보를 보내도록 변경한 것이다. 이 SNI를 사용하게 되면 하나의 웹 서버에서 여러 도메인의 웹사이트를 서비스하는 경우에도 인증서를 사용한 HTTPS를 활성화시킬 수 있다.

HTTPS에서 사용되는 TLS (Transport Layer Security) Handshake 프로토콜에서 TLS[7]는 Client와 Server 간의 통신을 이루기 위해서 Client가 Server에 ClientHello 메시지를 Server에 전송하고 Server는 이에 대한 답변으로 ServerHello라는 응답을 전송하게 된다. 이러한 절차는 다음의 <그림 1>과 같다.



<그림 1> TLS 협상과정

ClientHello 메시지를 서버에 전송하는 과정에서 SNI 필드 값을 포함하게 된다. 이 SNI는 TLS 프로토콜 상에서 접속하고자 하는 호스트 이름을 포함하는 평문값이다. 따라서 이 SNI 값을 통해서 HTTPS에서 동일 IP 주소와 TCP 포트를 사용하는 서버에서 다수의 인증서를 사용할 수 있게 해주고 이로 인해 모든 사이트가 같은 인증서를 사용하지 않아도 동일 서버에서 여러 개의 HTTPS 사이트를 운영할 수 있게 한다. 그러나 보안측면에서는 SNI 필드 값을 평문으로 전송하므로 이 데이터가 전송되는 구간에 있는 장비들에서는 패킷을 캡처해서 인터넷 사용자가 접속하려는 웹사이트를 알 수 있다.



<그림 2> SNI 필드를 이용한 접속차단

2.2 SNI 필드를 이용한 접속차단 방법

기존에 유해사이트를 차단하는 방법은 인터넷 사용자가 웹브라우저 주소창에 URL을 입력하면 DNS[8]를 통하여 해당 IP 주소로 연결하게 되는데, 만약 정부가 지정한 불법 유해사이트일 경우 경찰청 경고 사이트(warning.or.kr) 화면으로 자동 연결하게 된다. 그러나 인터넷에서 전송되는 데이터를 암호화하여 송수신하는 프로토콜인 HTTPS를 사용함에 따라 기술적으로 차단이 어려운 문제가 발생하게 되었다.

이러한 문제를 해결하기 위해 제안한 방식이 SNI[9, 10] 필드 차단 기술이다. 데이터가 암호화되기 전에 평문으로 전송되는 TLS의 ClientHello 메시지에 있는 SNI를 확인하면 인터넷 사용자가 어느 사이트에 접속하려고 하는지 알 수 있으므로 이를 차단목록 DB에 있는 웹사이트 주소이면 국내 ISP에서 해당 인터넷 접속을 차단하는 방식이다.

SNI 필드는 기존에도 평문으로 전송되는 데이터로 해당 데이터를 이용해 어느 사이트로 접속하는지 알 수 있었으나 이를 이용하여 인터넷 접속을 차단함으로 인터넷 사용자들이 접속하는 사이트 정보의 활용에 대한 보안측면의 우려가 증가하고 있다. 따라서 이에 대한 익명성 보장 제공방안의 연구가 필요한 실정이다.

2.3 ESNI(Encrypted SNI)

TLS 표준에는 SNI 암호화가 없어 SNI 필드가 평문 형태로 전송된다. 이로 인해 제 3자에게 쉽게 노출이 되어 보안 문제가 생기기 때문에 TLS에 SNI의 암호화 규격을 추가하는 문제는 오랜 기간 논의가 되어 왔다. 2018년 7월 2일에 Apple, Cloudflare, Fastly, Mozilla에 의해 작성된, TLS 1.3을 전제로 한 확장 규격으로서의 SNI 암호화 규격의 초안 문서가 IETF에 제안되었다.

ESNI 구현은 클라이언트 브라우저에 서버의 공개키가 전달되는 시점을 DNS 통신 단계로 앞당겨서 서버와 연결하는 시점에 해당 공개키로 도메인이 암호화될 수 있도록 하는 것이다. 파이어폭스는 ESNI 구현이 DNS 통신의 암호화가 이루어지지 않는 상황에서는 별 의미가 없다는 점에 의해 ESNI가 작동하려면 DNS over HTTPS[11]가 활성화되어 있을 것을 요구하고 있다. 웹사이트가 TLS 1.3을 지원하고 ESNI가 구현된 서버 프로그램을 사용하면 SNI 패킷에 기록된 도메인 또한 암호화되므로 차단을 회피할 수 있으나, 아직 정식 표준으로 채택되지 않은 초안 단계이기 때문에 적용되는 곳이 많지 않다는 어려움을 가지고 있다.

Ⅲ. 익명성 제공 사이트 차단 모델

본 논문에서는 법률을 기반으로 유해 사이트를 차단하는 과정에서 SIN가 평문으로 전송되어 인터넷 사용자가 이용하는 접속 사이트에 대한 정보가 공개됨으로 발생할 수 있는 정보 노출을 차단하면서 유해 사이트를 차단할 수 있는 방안에 대한 연구를 수행하였다.

3.1 제안 모델

일반적으로 인터넷 이용자를 식별할 수 있는 방법은 사용자의 IP 주소 값의 확인을 통해 알 수 있으므로 어느 사용자가 어느 사이트에 접속하는지에 대한 익명성을 제공하기 위해서는 SNI 정보뿐만 아니라 IP 주소에 대해서도 안전한 조취를 취해야 한다. 따라서 <그림 2>의 국내 ISP에서 웹사이트를 차단하는 절차 중 익명성 제공방안을 제시하고자 한다.

- Hash 값 생성

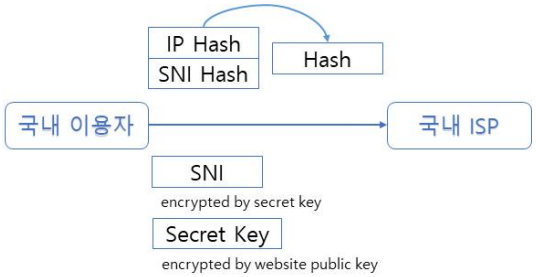
인터넷 사용자가 웹사이트에 서비스를 요청할 때 기존의 패킷이외에 IP 주소의 Hash 값과 SNI의 Hash 값을 생성하고, 이 두 Hash의 값을 이용하여 새로운 Hash 값을 생성한다.

- 비밀키 생성 및 암호화

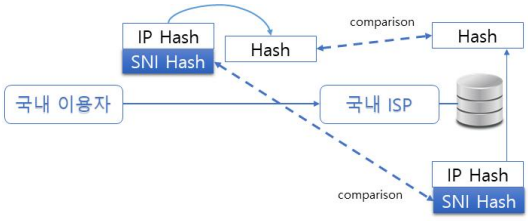
인터넷 사용자의 웹브라우저에서 비밀키(비대칭키)를 생성하여 서비스를 요청하는 웹사이트의 공개키(대칭키)로 비밀키를 암호화한다.

- ISP에서의 차단 목록 비교

ISP에서 유해 사이트를 차단하기 위해 차단 목록과 비교하는 과정에서는 <그림 3>에 제시된 바와 같이 인터넷 사용자가 추가로 전송한 데이터만 사용하도록 제한한다. 익명성을 제공하기 위해 IP 주소값이 Hash



<그림 3> 인터넷 사용자 전송 정보



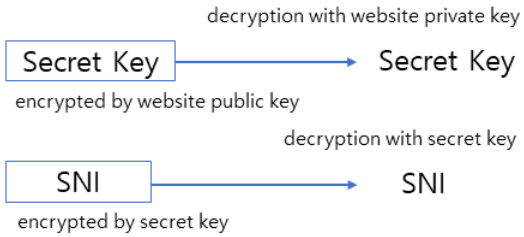
<그림 4> 차단 목록 비교

로 되어 있으며, 차단 목록 해당여부를 분석하기 위해서는 <그림 4>와 같이 SNI Hash 값과 차단 사이트 목록의 도메인 이름들을 Hash 값으로 만든 목록과의 비교를 통해 차단여부를 결정하게 된다. 따라서 ISP에서는 인터넷 사용자가 접속하려는 웹사이트가 유해 사이트인 경우 해당 웹사이트를 차단하도록 하지만 어느 사용자가 요청한 요청인지는 알 수 없다. 또한 데이터의 무결성을 점검할 수 있는데, 차단목록 DB에 있는 SNI Hash값을 기존의 SNI Hash 값과 대체한 후 IP 주소의 Hash 값과 SNI의 Hash 값으로 생성한 Hash 값과 인터넷 사용자가 보내온 Hash 값의 비교를 통해 데이터의 위·변조 여부를 판별할 수 있다.

- 해외 웹 서버에서의 동작과정

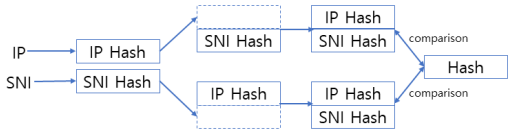
해외 웹 서버에서는 ISP를 통해서 전송받은 데이터의 무결성 검토 및 암호화된 SNI 필드의 복호화를 통해 그 내용을 확인해야 한다. 먼저 SNI 필드의 복호화는 인터넷 사용자가 생성한 비밀키로 암호화 되어 있으며, 또한 그 비밀키는 웹사이트의 공개키로

암호화 되어 있으므로 웹사이트의 사설키로 비밀키를 획득할 수 있으며, 이 비밀키를 획득하면 SNI 필드 값을 복호화 할 수 있다. 따라서 웹 서버에서는 해당 웹사이트 주소 정보를 확인할 수 있다. 이에 대한 설명은 다음의 <그림 5>와 같다.



<그림 5> SNI 필드 복호화

웹 서버에서 무결성 및 출처인증 검사는 <그림 6>과 같다. 무결성 검증은 복호화 된 SNI 필드를 이용하여 Hash 값을 생성한 후 전송받은 IP Hash 값과 생성한 SNI Hash 값을 이용해 새로운 Hash 값을 생성해 전송받은 Hash 값과 비교하여 무결성을 점검할 수 있다. 또한 전송받은 패킷의 Source IP 주소 값에 대한 Hash 값을 생성하고 복호화 한 SNI 필드 값을 이용해 생성한 SNI Hash 값을 사용해 새로운 Hash 값을 생성해 전송받은 Hash 값과 비교함으로 출처인증을 수행할 수 있다.



<그림 6> 무결성 및 출처인증 검사

3.2 분석 결과

기존의 HTTP 프로토콜에서는 DNS 정보를 활용하여 유해 사이트 도메인 리스트에 해당하는 사이트를 차단하는 방식을 이용하였다. 그러나 HTTPS가 일반화됨에 따라 기존의 방식으로는 유해 사이트 차단에 어려움이 발생하게 되어 SNI 필드 값을 이용해 유해 사이트를 차단하고 있으며 본 논문에서는 유해 사이트 차단이 수행되면서도 안전하게 인터넷 사용자의 익명성을 제공할 수 있는 모델을 제시하였다. 기존에 사용되던 프로토콜과 제안한 모델과의 성능 비교를 수행한 내용은 다음의 <표 1>과 같다.

<표 1> 기존 모델과의 성능 비교

기능	HTTPS	제안 모델
ISP에서 유해 사이트 차단 시 사용자에 대한 익명성 제공	X	○
ISP에서 IP주소와 SNI 필드 값의 무결성 검증	X	○
웹 서버에서 SNI 필드와 IP 주소에 대한 무결성 검증	X	○
웹 서버에서 전송받은 메시지에 대한 출처인증	X	○

성능비교 결과 <표 1>에서 제시한 바와 같이 유해 사이트로 판단되어 차단되는 인터넷 사용자들에 대한 익명성 제공뿐만 아니라 무결성과 출처인증까지도 수행할 수 있어 인터넷 사용자의 신원노출을 막고 유해 사이트의 차단 및 안전한 메시지의 전송을 수행할 수 있다.

Ⅳ. 결론

유해 사이트의 증가에 따라 사회적으로 많은 문제가 발생하고 있다. 따라서 정부에서는 이러한 문제를 해결하고자 유해 사이트에 대해 웹 페이지 접속을 차단하는 활동을 법률에 근거하여 수행하고 있다. 그러나 HTTP에서 HTTPS 프로토콜로 변화됨에 따라 기존의 방식으로는 유해 사이트의 차단이 어려워졌다. 이에 대한 대책으로 HTTPS 프로토콜에 있는 TLS

Handshake에서 평문으로 전송되는 SNI 필드를 이용한 유해 사이트를 차단 방식이 도입되었다. 그러나 SNI 필드를 이용하는 방식은 인터넷 사용자들에 대한 감시 혹은 접속하는 사이트에 대한 정보노출 이라는 우려를 발생시킴에 따라 본 논문에서는 이러한 문제를 해결하고자 유해 사이트를 차단하면서 인터넷 사용자들에게는 익명성을 제공하는 방안에 대한 연구를 수행하였다. 제안한 모델에서는 이용하는 웹사이트에 대한 익명성 제공뿐만 아니라 무결성과 출처 인증을 수행할 수 있어 안전하게 사용할 수 있는 방안을 제시하였다.

단, 본 연구에서는 유해 사이트 차단 수행의 옳고 그름에 대한 분석을 수행한 것이 아니라 유해 사이트 차단시에 익명성을 제공하는 방안에 대한 연구를 수행하였으며, 현재 이러한 기능을 수행할 수 있도록 하는 ESNI 기술이 개발되고 있으나 아직 표준화되지 않았고, 이 기술을 사용할 수 있는 환경도 우리가 대부분 많이 사용하는 익스플로러나 크롬에 제공되지 않아 추후 계속적인 연구가 필요한 상황이다.

참고문헌

[1] Mathrani, Anuradha, and Massoud Alipour, "Website Blocking Across Ten Countries: A Snapshot," PACIS. 2010, p. 152.

[2] Danaher, Brett, Michael D. Smith, and Rahul Telang, "The effect of piracy website blocking on consumer behavior," Available at SSRN 2612063, 2018.

[3] 윤여생, 유진호, "불법유해정보 법・제도 동향 분석," 정보보호학회지, 22(3), 2012.5, p. 25-36.

[4] 최미정, 진창규, 김명섭, "HTTP 트래픽의 클라이언트측 어플리케이션별 분류," 한국통신학회논문지, 36(11), 2011.11, pp. 1277-1284.

[5] 김성민, 박준상, 윤성호, 김종현, 최선오, 김명섭, "SSL/TLS 기반 암호화 트래픽의 서비스 식별 방법," 한국통신학회논문지, 40(11), 2015.11, pp. 2160-2168.

[6] 짠송닷푹, 이창훈, "SSL/TLS 공격에 대한 신규 대응 방안," 한국전자거래학회지, 22(2), 2017.5, pp. 169-185.

[7] Rescorla, Eric. The transport layer security (TLS) protocol version 1.3. No. RFC 8446. 2018.

[8] 김광섭, 박영길, 노승환, 김봉현, "DNS 정보 검색 연동 기법을 이용한 침해 사고 예방 시스템 설계," 한국정보통신학회논문지, 16(9), 2012.09, pp. 1955-1962.

[9] Shbair, Wazen M., et al., "Efficiently bypassing SNI-based HTTPS filtering," 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE, 2015, pp. 990-995.

[10] Shbair, Wazen M., et al., "Improving sni-based https security monitoring," 2016 IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW). IEEE, 2016, pp. 72-77.

[11] Hoffman, P., and P. McManus. Dns queries over https (doh). No. RFC 8484. 2018.

■ 저자소개 ■

김 태 경
(Kim Taekyung)

2017년 9월~현재
명지전문대학
인터넷응용보안공학과 교수
2008년 3월~2017년 8월
서울신학대학교 교수
2006년 3월~2008년 2월
서일대학 정보전자과 교수
2005년 8월 성균관대학교 전기전자 및
컴퓨터공학과(공학박사)

관심분야 : 네트워크보안, IoT 보안,
개인정보보호
E-mail : tkkim@mjc.ac.kr

논문접수일 : 2019년 02월 27일
게재확정일 : 2019년 03월 05일